E-Government

Enterprise Directory

An Architectural Overview
For Implementing
The Enterprise Directory

Prepared By

Specialized Technical Services - STS

Table of Contents

1.0 Document Control

1.1 Document History

Company Name	**Specialized Technical Services STS**		
Project	**E-Government Enterprise Directory**		
Approval 1	**Momen Al-Ashram**		**MA**
Approval 2	**Feras Mustafa**		**FM**
Approval 3	**Hassan Abukuppeh**		**HA**
Revision No.	**0**	**Date**	**Sept.28.2002**

1.2 Internal Distribution list

Entity or Person's Name	Mean of Delivery	Date
Mr. Ayman Mazahreh	E-mail	Sept.28
Mr. Sadeq Shunnar	E-mail	Sept.28
Mr. Hisham Varoqua	E-mail	Sept.28
Mr. Eyad Soboh	E-mail	Sept.28
Mr. Daoud Abbod	E-mail	Sept.28

1.2 External Distribution list

Entity or Person's Name	Mean of Delivery	Date
Mr. Fadi Mare'	E-Mail	Sept.28
Mr. Abdel-Majeed Shamlawi	E-Mail	Sept.28

2.0 Introduction

2.1 Scope

This document addresses the Architecture design and deployment of the E-Government Enterprise Directory for the Government of Jordan as stated in the Enterprise Directory Scope Document. Windows 2000 Active directory will be the choice of directory service to be deployed.

2.2 Primary Goals for the Enterprise Directory?

We are implementing the Enterprise Directory Services for the Government of Jordan (GoJ) to achieve the following primary goals:

- To enables improved network and application security.
- As a database to store information such as people, phone numbers, addresses, etc.
- As a users point of access to locate resources and information.
- To authenticate and control user access to applications in the directory.

2.3 Proposal Dependencies

Our proposed solution depends on the following points being implemented for its coherence and completion, they are:

- Each of the six ministries (MOP, PM, MOF, MOIT, MOGA, and MOICT) must have the hardware needed to be a child domain, which is two domain controllers for each.
- All Client workstations and servers in each of the six ministries must join their new domain.
- Each of the six ministries will apply its own account policy.
- Child Domain data and backup will be the responsibility of each ministry.
- A single Global Address List is needed for all **GoJ** employees.
- Each of the six ministries will have full Administrative control of itself.
- Security boundaries are needed between ministries.

2.4 Long term commitment

Another important point to be considered is ***future interoperability*** with other directory services. The government of Jordan by committing itself to a Microsoft Active Directory is not implementing a short-term solution. Microsoft Active Directory and Metadirectory provide interoperability with other product's directories and Metadirectories to better serve future more complex and demanding business environments.

The choice for Active Directory is a balanced long-term solution for the Government of Jordan.

3.0 Why Windows 2000 Active Directory Services.

3.1 Introduction

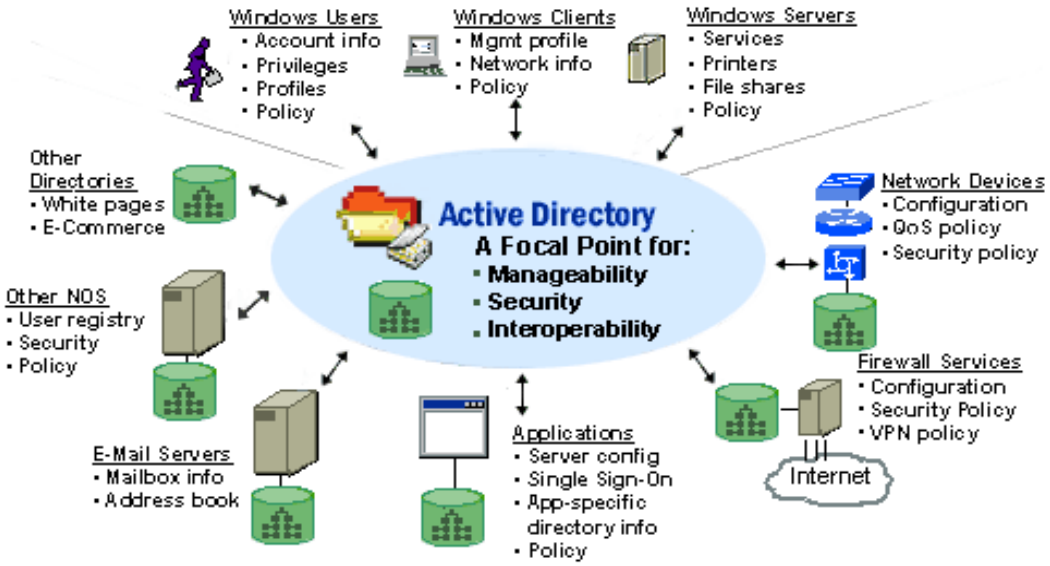
Today, networked computing is more important than ever for businesses to remain competitive. As a result, modern operating systems require mechanisms for managing the identities and relationships of the distributed resources that make up network environments. A directory service provides a place to store information about network-based entities, such as applications, files, printers, and people. It provides a consistent way to name, describe, locate, access, manage, and secure information about these individual resources.

Further, a directory service acts as the main switchboard of the network operating system. It is the central authority that manages the identities and brokers the relationships between these distributed resources, enabling them to work together. Because a directory service supplies these fundamental network operating system functions, it must be tightly coupled with the management and security mechanisms of the operating system to ensure the integrity and privacy of the network. It also plays a critical role in an organization's ability to define and maintain the network infrastructure, perform system administration, and control the overall user experience of a company's information systems.

3.2 What Is Active Directory?

Active Directory is an essential and inseparable part of the Windows 2000 network architecture that improves on the domain architecture of the Windows NT® 4.0 operating system to provide a directory service designed for distributed networking environments. Active Directory lets organizations efficiently share and manage information about network resources and users. In addition, Active Directory acts as the central authority for network security, letting the operating system readily verify a user's identity and control his or her access to network resources. Equally important, Active Directory acts as an integration point for bringing systems together and consolidating management tasks.

Combined, these capabilities let organizations apply standardized business rules to distributed applications and network resources, without requiring administrators to maintain a variety of specialized directories.



Active Directory provides a single point of management for Windows-based user accounts, clients, servers, and applications. It also helps organizations integrate systems not using Windows with Windows-based applications, and Windows-compatible devices, thus consolidating directories and easing management of the entire network operating system. Companies can also use Active Directory to extend systems securely to the Internet. Active Directory thus increases the value of an organization's existing network investments and lowers the overall costs of computing by making the Windows network operating system more manageable, secure, and interoperable.

Active Directory is the first enterprise-class directory service that is scalable, built from the ground up using Internet-standard technologies, and fully integrated with the operating system. In addition to providing comprehensive directory services to Windows applications, Active Directory is designed to be a consolidation point for isolating, migrating, centrally managing, and reducing the number of directories that companies have. This makes Active Directory the ideal long-term foundation for corporate information-sharing and common management of network resources, including applications, network operating systems, and directory-enabled devices.

3.3 A Step above the rest

A good way for organizations to make directory decisions is to identify the roles that they envision for directory services within their organization and compare how well that Directory service supports each role. Based on the arguments, Microsoft Active Directory shows that it is:

- A better directory for network resource management.
- A better directory for Internet applications such as e-commerce and extranets.
- A better directory for applications, and has more support from important infrastructure and application vendors.
- A better platform for directory consolidation and centralized directory management.
- The only Directory for implementing Exchange 2000.
- Will meet the customer requirements of a multi-purpose directory service much better than other directories. This makes Active Directory the best long-term directory service choice.

4.0 Data Collection

The participating entities in the initial roll out are:

1. Prime Ministry (PM)
2. Ministry of Industry and Trade (MoIT)
3. Ministry of Planning (MoP)
4. Ministry of Information and Communication Technology (MoICT)
5. Ministry of Finance (MoF)
6. Municipality of Greater Amman (MoGA)

4.1 Data collection strategy

A data collection strategy has been implemented. It aims at collecting current data for three major categories. They are:

1. Network Infrastructure and Network Operating Systems
2. Organizational Structure
3. Personnel Information

Forms have been designed and provided to each ministry to fill out for each category. Many of which have already been turned in to our team.
Please refer to Document titled "Data Collection Overview Document" included under appendix B

******After reviewing all the data turned in to us, we have summarized the followings:***

4.2 Ministries Current Domain Infrastructure

The ministry of Information and communication Technology (MoICT) is the only Ministry, of the 6 ministries; that has a Windows 2000 Domain infrastructure. All other ministries have a Unix infrastructure, Novel, or no infrastructure at all.

4.3 Clients stations and Operating systems

All clients' workstations run Operating systems under Microsoft platforms. They are either:

1. Windows 95
2. Windows 98
3. Windows Me
4. Windows 2000 Professional
5. Windows XP Professional

4.4 Servers and Operating systems

All ministries have servers that perform many roles. These servers are comprised of the following operating systems.

1. Unix Servers
2. Novel Netware Servers
3. Sun Solaris Servers
4. Windows NT 4.0 Servers
5. Windows 2000 Servers

4.5 Servers and Their Roles

Servers in the participating ministries are performing a variety of roles and running several types of in-house or vendor designed applications. Some of these roles are:

1. Exchange Servers
2. E-mail Servers
3. Application Servers
4. File and Print servers
5. Other types of Servers

4.6 Personnel, Objects and Organizational Resources

We currently have records for the personnel and organizational structure for the ministries involved. This information will provide the source for the Data Entry team to enter the information into the new designed Active Directory.

5.0 Data Entery Strategy

5.1 Personnel Information

Once all of the data has been collected, a ***Data entry team*** will carry the responsibilities of entering this data into the Enterprise Directory.

5.2 Organizational Structure

5.2.1 The Six ministries

In this document, the proposed implementation of the Enterprise Directory would address the Organizational Structure as follows:

- The top of the Organizational Structure being the Ministry itself would be represented as a domain. See item 6.2.2
- Each of the six ministry's internal departments, as supplied by the ministries themselves, would be represented in their existing Hierarchical order. See Figure 6.4.2
- Each of the six ministry's internal Major departments, as supplied by the ministries themselves, would be represented by an OU (Organization Unit)
- A Child OU would represent each department within those major departments.
- This process is repeated until the 3 levels of departments are represented
- This process recommends a maximum of 10 levels

5.2.2 All other ministries

This document addresses the Organizational Structure migration for all other ministries as follows:

- The top of the Organizational Structure being the Ministry itself would be represented as an OU (Organizational Unit) within the Domain GoJ. See item 6.2.1
- Each of the ministries' internal departments, as supplied by the ministries themselves, would be represented in their existing Hierarchical order.

- A Child OU would represent each of the ministries' internal Major departments.
- A Child OU would represent each department within those major departments.
- This process is repeated until the 3 levels of departments are represented
- This process recommends a maximum of 10 levels

A ***Data entry team*** will carry the responsibilities of entering this data into the Active Directory

5.3 Network Infrastructure Migration

5.3.1 Clients workstations

The Windows 2000 domain structure design for the Active Directory includes a role out for all client workstations. The client's role out will implement a Windows 2000 professional Operating system for all client workstations.

- All clients operating Windows 2000 and Windows XP professional have built in services to access the domain and the Active Directory.
- All clients operating Windows 2000 and Windows XP professional can access all Window NT 4.0 servers.
- For clients to Access UNIX servers, Services for UNIX can be installed on the clients.
- For clients to Access NOVEL NETWARE servers, Client Services for NETWARE can be installed. Windows 2000 also provides the NWLink protocol, which is Microsoft version of the IPX/SPX protocol running on the NOVEL NETWARE servers.
- As for the SUN-SOLARIS servers running the E-mail services, they will be replaced with the Exchange 2000 running on the Windows 2000 servers.

5.3.2 Servers

All existing servers can and will be incorporated into the new Infrastructure, except for the SUN-SOLARIS servers running the E-mail services. Those

servers would have to be replaced by the new Infrastructure with the Exchange 2000, or can be used for other applications.

- For Windows 2000 servers to access the UNIX servers, Services for UNIX can be installed
- For Windows 2000 servers to access the NOVEL NETWARE servers, Gateway services for Netware can be installed.

Note: A detailed migration plan will be presented as soon as all the details have been identified. It will come under a separate document addressing the detailed roll-out.

6.0 Proposed Architecture Designs

6.1 Design Foundation (DATA CENTER)

6.1.1 Root Domain Design

The design will be based on an empty root domain structure. This will allow for flexibilities in areas like:

1. Child domains can be created under this domain for needed expansion.
2. The ability to maintain a naming convention. A ministry does not have to be named under another ministry's name; it can have its own fully qualified domain name.

One of the primary purposes of implementing AD is to support Exchange 2000 as well as other applications. Since the boundary of the Exchange 2000 organization is the Active Directory Forest, and since there is a need to have single Global Address List, a single Active Directory Forest with an empty root domain named **GOV.** will be created.
For fault tolerance, at least two domain controllers will be created in that root domain, **GOVDC1** and **GOVDC2**. Each Domain controller will have ***DNS*** service with Active Directory Integrated Zones;

- **GOVDC1** will point to itself as the alternate DNS server and to **GOVDC2** as the preferred DNS server.
- **GOVDC2** will Point to its self as the alternate DNS server and to **GOVDC1** as the preferred DNS server.

GOVDC1 will be a global catalog server (GC), and will host the Schema master and Domain Naming master roles. This means that any update to the schema, must be made from **GOVDC1**.

GOVDC2 will host the PDC Emulator master, RID master, and Infrastructure master.

Note: Operation Master Roles can be easily moved between domain controllers in the domain.

The Storage Location for **GOVDC1** and **GOVDC2** Active Directory database will be hosted on single RAID5 Group on the SAN Storage, and the LOG files will be hosted on a RAID1 Group. See Figure 6.1.1 in Appendix A.

We strongly recommend that this **GOV.** Domain would only contain the Administrator account renamed and with minimum password length of 18 characters.

6.1.2 Single Child Domain GoJ.

A child domain named **GoJ.GOV** (Government of Jordan) with a NetBIOS name of **GoJ** will be created in the data center site. See Figure 6.1.2 in Appendix A.

For fault tolerance, at least two domain controllers will be created in this domain**; GoJDC1** and **GoJDC2.** Each Domain controller will have ***DNS*** service with Active Directory Integrated Zones;

- **GoJDC1** will point to itself as the preferred DNS server and to **GoJDC2** as the alternate DNS server.
- **GoJDC2** will Point to its self as the preferred DNS server and to **GoJDC1** as the alternate DNS server.

GoJDC1 will be a global catalogue server (GC). It will also host the PDC Emulator, RID master, and Infrastructure master for the Child Domain.

The Storage Location for **GoJDC1** and **GoJDC2** Active Directory database will be hosted on one RAID5 Group on the SAN Storage, and the LOG files will be hosted on a RAID1 Group.

6.2 Ministries Representations

6.2.1 Option 1: As Organization Units within GoJ

Ministries will each be represented as a single OU (Organization Unit) inside the single child domain .GoJ of the root domain .GOV.
See Figure 6.1.2

For each OU there will be a Delegated Security Group with Full Control permission on all the objects inside their own OU. This group will be responsible for daily tasks such as resetting users' passwords, adding computers to the domain, etc.

Users will logon to domain using UPN (i.e. username@GoJ.gov).

Pros,

- Minimal Hardware. No need for Servers.
- Less Administrative Overhead. There is only one domain to manage.
- Simple naming Convention. All are under one domain name.
- Centralized Administration.

Cons,

- Higher Network traffic If Users and domain controllers are not in the same location.
- No independent security boundaries. Since all ministries are represented by an OU, they are bound by the domain policy.
- Limited flexibility. The OU structure allows less flexibility than for say a domain.

6.2.2 Option 2: Multi Child Domains

A new child domain could be created for any of the ministries from the **GOV** Root domain.

See figure 6.2.2a and figure 6.2.2b for Optional Physical layout with regards to SAN Storage in Appendix A.
See figure 6.2.2c for Logical Layout

Important: All other remaining ministries will remain accommodated for within the child domain GoJ as OU's

Each of these child domains must contain two domain controllers for fault tolerance; and the 2nd DC will be the global catalogue server.

Provided that the six ministries that were discussed in the initial role out participate, it would result in a total of seven (7) child domains under .GOV root domain. These domains will be as follows:

1- Prime Ministry (PM.GOV)

Two domain controllers will be created for **PM.GOV** domain named **PMDC1** and **PMDC2.** The NetBIOS Domain name will be **PM.**
Each domain controller will be a DNS with Active Directory Integrated Zones. Each domain controller will point to itself as the preferred DNS server and to the other domain as the alternate DNS server.
PMDC1 will be Global Catalog (GC) server and PDC emulator, and RID Master.

PMDC2 will be the Infrastructure master.
Users will logon to domain using UPN (i.e. username@pm.gov).

2- Ministry of Industry and Trade (MoIT.GOV)

Two domain controllers will be created for **MoIT.GOV** domain named **MoITDC1** and **MoITDC2**, the NetBIOS domain name will be **MoIT**.
Each domain controller will be a DNS with Active Directory Integrated Zones.
Each domain controller will point to itself as the preferred DNS server and to the other domain as the alternate DNS server.
MoITDC1 will be Global Catalog (GC) server and PDC emulator, and RID Master.
MoITDC2 will be the Infrastructure master.
Users will logon to domain using UPN (i.e. username@MoIT.gov).

3- Ministry of Planning (MoP.GOV)

Two domain controllers will be created for **MoP.GOV** domain named **MoPDC1** and **MoPDC2**, the NetBIOS domain name will be **MoP**.
Each domain controller will be a DNS with Active Directory Integrated Zones.
Each domain controller will point to itself as the preferred DNS server and to the other domain as the alternate DNS server.
MoPDC1 will be Global Catalog (GC) server and PDC emulator, and RID Master.
MoPDC2 will be the Infrastructure master.
Users will logon to domain using UPN (i.e. username@MoP.gov).

4- Ministry of Information and Communication Technology (MoICT.GOV)

Two domain controllers will be created for **MoICT.GOV** domain named **MoICTDC1** and **MoICTDC2**, the NetBIOS domain name will be **MoICT**.
Each domain controller will be a DNS with Active Directory Integrated Zones.
Each domain controller will point to itself as the preferred DNS server and to the other domain as the alternate DNS server.
MoICTDC1 will be Global Catalog (GC) server and PDC emulator, and RID Master.
MoICTDC2 will be the Infrastructure master.
Users will logon to domain using UPN (i.e. username@MoICT.gov).

5- Municipality of Greater Amman (MoGA.GOV)

Two domain controllers will be created for **MoGA.GOV** domain named **MoGADC1** and **MoGADC2**, the NetBIOS domain name will be **MoGA**.
Each domain controller will be a DNS with Active Directory Integrated Zones.
Each domain controller will point to itself as the preferred DNS server and to the other domain as the alternate DNS server.
MoGADC1 will be Global Catalog (GC) server and PDC emulator, and RID Master.
MoGADC2 will be the Infrastructure master.
Users will logon to domain using UPN (i.e. username@MoGA.gov).

6- Ministry of Finance (MoF.GOV)

Two domain controllers will be created for **MoF.GOV** domain named **MoFDC1** and **MoFDC2**, the NetBIOS domain name will be **MoF.**
Each domain controller will be a DNS with Active Directory Integrated Zones.
Each domain controller will point to itself as the preferred DNS server and to the other domain as the alternate DNS server.
MoFDC1 will be Global Catalog (GC) server and PDC emulator, and RID Master.
MoFDC2 will be the Infrastructure master.
Users will logon to domain using UPN (i.e. username@MoF.gov).

7- Government of Jordan (GoJ.GOV)

A child domain named **GoJ.GOV** (Government of Jordan) with a NetBIOS name of **GoJ** will be created in the data center site. See Figure 6.1.2 in Appendix A.

For fault tolerance, at least two domain controllers will be created in this domain**; GoJDC1** and **GoJDC2.** Each Domain controller will have ***DNS*** service with Active Directory Integrated Zones;

- **GoJDC1** will point to itself as the preferred DNS server and to **GoJDC2** as the alternate DNS server.
- **GoJDC2** will Point to its self as the preferred DNS server and to **GoJDC1** as the alternate DNS server.

GoJDC1 will be a global catalogue server (GC). It will also host the PDC Emulator, RID master, and Infrastructure master for the Child Domain.

The Storage Location for **GoJDC1** and **GoJDC2** Active Directory database will be hosted on one RAID5 Group on the SAN Storage, and the LOG files will be hosted on a RAID1 Group.
Users will logon to domain using UPN (i.e. username@GoJ.gov).

Pros,

- Unlimited scalability. For an example, a ministry can expand one of its departments to become a child domain of its own domain, and not be bound by the limited structure of a one domain for all.
- Each ministry can design and implement it's own security boundaries.
- Lower network traffic. Where traffic and replication is occurring within the site only.

Cons,

- More Hardware. You need Domain Controllers (Servers).
- More Administrative Overhead. A ministry is responsible for a whole domain and not just for an OU.

6.3 Sites and Site links

You can use sites to control:

- *Replication traffic*. When a change occurs in Active Directory, sites can be used to control how and when the change is replicated to domain controllers in another site.
- *Logon traffic*. When a user logs on, Windows 2000 attempts to find a domain controller in the same site as the workstation.
- *Requests to Global Catalog*. When a request to a Global Catalog is required, a user computer or a Domain Controller finds a Global Catalog in the local site.

6.3.1 Data Center Site

A Data Center Site will be created and will host the Domain Controllers in the **GOV** and **GoJ.GOV** Domains mentioned in 6.1.1 and 6.1.2.

See Figure 6.3.1 in Appendix A.

6.3.2 Option 1: Multiple Sites with Site links

For each ministry to be represented in it's own child domain, a single site would be created. From item 6.2.2
See Figure 6.3.2 in Appendix A.

Each site will be linked with one or more subnets depend on the number of subnets in each Ministry.
A site link connector will connect each Ministry site with the Data Center site. A Bridgehead server will be assigned to the second domain controller in each ministry, and this bridgehead server will connect to the **GoJDC2** in the Data Center site. The site link cost will be set to its default (100).

Pros,

- Optimized network traffic (compressed replication traffic).
- Within site Authentication.

Cons,

- More administrative overhead

6.3.3 Option 3: A Single Site for all

Place all domain controllers from all domains in the Data Center Site.
See figure 6.3.3 in Appendix A.

In this option, Administrators will connect to their respective domain controllers using Terminal Services (Remote Administration Mode) or by installing the Windows 2000 Administrator Tools on a Windows 2000 Professional workstation located in their ministry.

Pros,

- DCs can query each other faster.
- Less administrative overhead

Cons,

- Uncontrolled and high intra-site traffic.
- High authentication traffic.

6.4 Organizational Units (OU's)

The use of OU's in Windows 2000 Active Directory organizes the domain resources and simplifies the administration and management of users or objects in that domain.

6.4.1 OU Structure for Single-child Domain

This structure corresponds to option 1 in item 6.2.1

Since we will operate under a single child domain (**GoJ.GOV**), the first set of proposed OUs will have to reflect each ministry as a single OU. Within each corresponding ministry OU another set of child OUs will exist to mirror the Organizational Structure already existing at each ministry. The primary function of these child OUs will be to group and organize the departments and units for each ministry, and to delegate administrative tasks for managing user accounts. OU's are also a great place to apply Group policy.

6.4.2 OU Structure for Multi-child Domains

This structure corresponds to option 2 in item 6.2.2

Since the multi-child domain option in 6.2.2 proposed a child domain for each ministry, therefore the OU structure within those child domains should mirror the Organizational Structure already existing at each Ministry. Here, the major use of OU will be to group and organize the departments and units for each ministry, and to delegate administrative tasks for managing user accounts.

See Figure 6.4.2 in Appendix A.

Important: All other ministries will remain accommodated for within the child domain GoJ as a separate OU representing each additional ministry. See figure 6.2.2a and figure 6.2.2b in Appendix A.

6.5 Networking Services

The Networking services are a fundamental part of the Enterprise architecture that can have a very serious effect on the performance of the services of the data center if they are not correctly managed. This section provides information on the following Networking services:

- DNS
- WINS
- DHCP

6.5.1 DNS

DNS is an acronym for Domain Name System, which is a hierarchical distributed database used to locate domain names on public and private TCP/IP networks. DNS provides a service for mapping DNS domain names to IP addresses, and vice versa. This service allows users, computers, and applications to query the DNS about remote systems by fully qualified domain names rather than by IP addresses.

A DNS server will be installed in the Data Center and in each domain created thereafter, and will be installed on each DC (Domain Controller) in those domains. All DNS servers will be Active Directory Integrated Zones.
Refer back to section 6.1

6.5.2 WINS

WINS, an acronym for Windows Internet Name Service, was developed by Microsoft to perform name registration, resolution, and deregistration using unicast datagrams to NetBIOS name servers.
WINS allows a network naming system to work across routers without LMHOSTS files, thereby restoring the dynamic nature of NetBIOS name resolution and allowing the system to work seamlessly with DHCP. For example, when dynamic addressing through DHCP creates new IP addresses for computers that move between subnets, the WINS database will track the changes automatically.

A minimum of one WINS server will be placed in each ministry, and will be installed as a member server. Please refer to section 6.12.2

6.5.3 DHCP

Dynamic Host Configuration Protocol (DHCP) is an extension of the Boot Protocol (BOOTP) that enables clients to obtain TCP/IP addresses

automatically. DHCP is a networking service provided with Microsoft Windows 2000 Server. The Microsoft DHCP service centralizes and manages the allocation of global and subnet-specific TCP/IP parameters to computers configured to use DHCP.
A minimum of one DHCP server will be placed in each ministry, and will be installed as a member server.

6.6 Schema / Arabic Language Support

The Active Directory *schema* contains the definitions of all objects, such as computers, users, and printers that are stored in Active Directory. In Windows 2000, there is only one schema for an entire forest, so that all objects created in Active Directory conform to the same rules.

6.6.1 Schema Extension

The final visualization of the Active Directory structure in order for it to include Arabic language attributes, amongst other reasons will force an extension of the Schema.

A list of attributes was decided on during the workshop held at STS on August 22nd, 2002. This list includes two sets of attributes, one for the OU's and department and one for the Users class. They can be found in **Appendix B**

Any modifications to the schema should be seriously considered before it is applied. For once a new class or attribute is added to the schema, it can be only be deactivated, but not removed. Moreover, an incorrect update to the schema can possibly cripple Windows 2000 Domain environment. The Active Directory is the heart of a Windows 2000 network and should be treated as such. Therefore, we recommend assigning a **Schema Modification Committee** that will review and approve any changes to the schema before it is done.

6.6.2 Arabic Language Support

Active Directory is the core feature of Windows 2000 operating system. All domain resources will be represented in the AD, like users, groups, folders, computers and any other kind of accounts.

To enable the multi language support for the Windows 2000 platform, **UNICODE** pages is used instead of the old **ANSI** code pages. Active Directory, as part of Windows 2000 platform, uses the **UNICODE** in all its components, and therefore supports Arabic language.

This Arabic language attributes addition will be implemented as follows:

- We will extend the schema to accommodate the Arabic attributes for every dual-language attributes.
- Those attributes will be created and stored in English in the AD
- An application will abstract the English name of the attribute and display it for the user in Arabic.
- The attributes will be Unicode strings; therefore they will hold Arabic values.
- Any queries that will be requested for any Arabic values will be performed against those attributes.

As for the search engine, the hit will be done on the root Global Catalog that will hold replica of all the searchable attributes in the whole government forest, that solution will enhance performance significantly, since we will avoid referral chasing in our application.

6.7 Active Directory Size

The estimated hardware specifications required for supporting the Active Directory design for the Data Center and each of the Six Ministries Domains is obtained by using the **AD Sizer** tool. The AD Sizer takes in consideration, the number of domains, sites, site links, number of users per domain and the WAN topology and then comes up with a suggested hardware configuration.

In the case of single child domain, with each ministry represented as an OU, the following hardware configuration is suggested based on **GoJ.GOV** Active Directory design:

AD database size	1.5 GB (average size)
GC database size (Global Catalog servers only)	2.5 GB (average size)

Table 1. GoJ.GOV Domain Controller Database Sizing

As for the disk storage, the Active Directory Database (**NTDS.dit**) should be stored on a RAID5 Group on the SAN Storage. The log files for this Database should also be stored on a RAID1 Group on the SAN Storage.

In the case of multiple child domains, with each ministry having it's own child domain, the following hardware configuration is suggested:

CPU	Pentium III 700 MHz
Ram	512 Mb
AD database size	600 MB (average size)
GC database size (Global Catalog servers only)	2.5 GB (average size)

Table 2. MoF.GOV Domain Controller Hardware Sizing

And as for the disk storage, the Active Directory Database (**NTDS.dit**) should be stored on a RAID5, and the log files, optionally stored on a RAID1 for each DC.

6.8 User Naming Convention

Implementing an AD Naming Convention for the Government of Jordan, must articulate the diversity and the culture of its employees. This culture as in the community it represent includes many similar and often the same family or last name. Therefore, the following naming convention was agreed upon during the Workshop at STS on August 22nd, 2002.

This naming convention will be used in the UPN form.

1st name.2nd initial.3rd initial.last name@moict.gov.jo
1st name.2nd initial.3rd initial.last name@GoJ.GOV

For example, an employee with a name of: Feras Saleem Ibrahim Mustafa would have the following UPN: feras.s.i.mustafa@GoJ.GOV

6.9 Backup and Restoration

The backup and restoration policies and responsibilities are discussed below. Backup and restoration policies are dependent on server location and WAN connections and could further be modified.

6.9.1 Data Center Site

A dedicated server must be installed with a sole responsibility of baking up all other servers and the SAN Storage located at this site.

We recommend using ***Veritas*** - **BackupExec** with the following Agents:

- Open File Option Agent.
- Exchange 2000 Option.
- SAN Shared Storage Option.

6.9.2 Ministries Sites

Each Ministry Domain Administrator will be responsible to backup the Domain Controllers at his site. The backup scheme should be full backup daily, starting from Sunday till Thursday.

The backup should include the Boot partitions and the System partition. In addition to the Systems State Data, which includes system startup files, system registry, COM+ class registration database, File Replication service (the SYSVOL directory), Certificate Services database (if it is installed),

Domain Name System (if it is installed), Cluster service (if it is installed) and the Active Directory database.

6.9.3 Restoring Active Directory

There are two ways to restore Active Directory. The first is to reinstall Windows 2000 and Active Directory, and then let normal replication repopulate Active Directory through the normal replication process. The other way is to restore Active Directory from a backup. The first method restores Active Directory to the current state with respect to its current replica partners. The second method restores Active Directory to a previously known state.

6.10 Active Directory Objects Security

Active Directory objects have security settings similar to security settings for file system objects on partitions using the NTFS file system. These permissions are different from those placed on file system objects, in that their inheritance attributes can be applied to subordinate objects based on the object type. See Figure 6.9 in Appendix A.

Management of user account properties can be delegated. Windows 2000 also offers more granular access control by controlling access to specific attributes within a particular object. For example, an object called "user" may contain attributes such as name, phone number, manager, department name, and telephone. Access may be limited to any of these attributes. So if we do not want all users on the system to be able to see the telephone numbers of other users, we can restrict access to the telephone attribute so that only management or human resources have access. Likewise, Windows 2000 object permissions include some items that may be qualified as privileges, such as the 'reset password' user object permission that can be set in the Active Directory.

6.10.1 Account Policy

To ensure an acceptable level of security for the Passwords and the Logon process, a user account policy for each domain in the GOV Forest will be defined as follows:

Password Policy:

- Minimum Password length is: 8 characters.
- Maximum Password length is: 14 characters.
- Minimum Password Age is: 0 days.
- Maximum Password Age is: 42 days.

Lockout Policy:

- Lockout duration is: 8 hours
- Lockout threshold is: 5 invalid attempts.
- Reset lockout counter after: 30 minutes.

Note: When you configure account policies (such as password policies and account lockout policies) in Active Directory, remember that Windows 2000 allows only one domain account policy per domain. Group Policy that is associated with one domain does not automatically propagate to other domains in the forest.

6.11 Administrative Distributions

This section will address the administrative diversity and how it would or could be distributed thru-out the Enterprise. One of the assumptions in the introductory part of this document is the need for some of the ministries to independently administer its own Tasks, personnel and security policies within their own boundaries. A list of proposed groups is included at the end of this section (6.11.5).

Enterprise Administration focal points can be summarized as follows:

6.11.1 Data Center

Administrators in this Root domain will be responsible for

- Setting the Account Policies for their own .GOV domain ***only***.

(However the only accounts to exist in this domain are the built in accounts).

- Setting all GPO's for their own .GOV domain ***only***.
- Back up and restorations for their own .GOV domain.

Important:

Members of the Administrators Group in the root domain also being members of the Enterprise Admin Group would be removed as members of any lower level administrators group. For example, by default, administrators in the root domain are automatically members of the administrators group in all child domains below them and all administrators groups in any OU within any of those child domains. In order to preserve the Independency of those child domains and OU's, those root domain administrators will be removed.

6.11.2 The .GoJ Child Domain

This Child domain of the .GOV root domain will be hosting many ministries. Those ministries will be represented as Organizational Units.

- Local Groups of users, from within each OU, would be assigned the Delegation of Authority for that particular OU and sub OU's.
- These groups would be named ***X*****Y** where ***X*** is the name of the OU, and **Y** is the function of that Group.
  For example: A group for only creating and modifying users accounts in the Ministry of Health would be called ***MoHaccounts*** Group, a group for only creating and modifying computer accounts would be ***MoHcomps*** Group and so forth.
- Users in one group can also be members of other groups.
- Users in these groups will be able to remotely administer their respective OU's using Terminal Services in Administration mode.
  Note: Terminal Services in administration mode only allows 2 concurrent sessions, therefore sessions should be scheduled and a limit must be set to prevent accessibility conflicts.

6.11.3 Other Child Domains

Each Child domain of the .GOV root domain would be hosting a single ministry.

Those ministries Administrators will be able to:

- Set the Account Policies for their own domain ***only***.
- Set all GPO's for their own domain ***only***.
- Back up and restore for their own domain ***only***.

6.11.4 Exchanges Global Address List GAL.

Exchange 2000 includes several default address lists. Users can use those lists as is or modify them to suit the needs of their organization. One of those lists is the Global Address List (GAL).

The GAL consist of all recipients in an organization:

- Mail Box
- Enabled Users
- Mail-Enabled Users
- Groups
- Contacts
- Public Folders

The Default GAL for the E-Government Enterprise will be present and replicated in all domains and child domains. However, Custom Address Lists (AL) can be created based on attributes of the recipients. This means that we can customize an AL for each Ministry or each OU. Access to these lists can be controlled thru Security Permissions and Access Rights from within each entity.

6.11.5 Administrative Groups

The following table lists possible administrative groups and their functions

Administrative Group	Purpose
Domain Admins	This group is the default domain admins group. Members of this group typically have complete control of the entire domain.
DNSAdmins	This group is created when DNS is installed. Members of this group have administrative rights to DNS within the domain.
Site Topology Admins	This group is manually created. Members of this group are delegated rights for maintaining the Active Directory Site Topology.
WINS Admins	This group is manually created. Members of this group are granted local administrative rights on the WINS servers.
DHCP Admins	This group is manually created and added to the local DHCP Admins group to grant administrative control over the DHCP servers.
Intranet Web Admins	This group is manually created and granted permissions on the IIS Web sites.
File Admins	This group is manually created and granted permissions to manage file services.
Print Operators	This group is automatically created by Windows 2000. This group is used to manage the print services within the domain.

6.12 Servers Roles & Hardware

6.12.1 Servers Roles

We can summarize the various roles of the servers thru out the Enterprise as follows:

- Domain Controllers
- DNS Servers
- WINS Servers
- DHCP Servers
- Global Catalog Servers
- PDC Emulators
- Domain Naming Master
- Schema Master
- RID Master
- Infrastructure Master

6.12.2 Servers Configurations and Specs.

This table will address the Servers Configurations and Hardware specifications for Servers placed in any ***child domain*** representing a ministry.

Domain Controller1	**Domain Controller2**	**Member Servers ***
DNS	PDC Emulator	WINS Server
Global Catalog	RID Master	DHCP
Schema Master	Infrastructure Master	
Naming Master		
Hardware Req.	**Hardware Req.**	**Hardware Req.**
PentiumIII 700 or Higher	PentiumIII 700 or Higher	PentiumIII 700 or Higher
512 MB Ram	512 MB Ram	512 MB Ram
10 GB Hard Disk	10 GB Hard Disk	10 GB Hard Disk

***:** In the case of having only two servers in a ministry, the WINS and DHCP roles can be shifted and placed on the second Domain Controller (DC2). However, we strongly recommend having a third server for these roles.

7.0 Conclusions

Having presented all the facts, we now present our concluded proposal as follows:

- **There will be a single parent domain (root) GOV**

  Refer to item 6.1.1 on page 16

- **There will be a child domain under the root domain to host the data of ministries not represented with own child domain GoJ.GOV**

  Refer to item 6.1.2 on page 16

- **These two domains will be in a single site (DATA CENTER)**

  Refer to item 6.3.1 on page 20

- **There will be multiple child domains under the parent domain; each could represent a participating ministry.**

  Example:

Prime Ministry	PM.GOV
Ministry of Industry and Trade	MoIT.GOV
Ministry of Planning	MoP.GOV
Ministry of Information and Communication Technology	MoICT.GOV
Municipality of Greater Amman	MoGA.GOV
Ministry of Finance	MoF.GOV

  Refer to item 6.2.2 on page 17

- **There will be multiple sites each to include the child domain of each ministry.**

  Refer to item 6.3.1 on page 20

- **There will be site links connecting each of the single child domains sites to the Data Center site.**

  Refer to item 6.3.1 on page 20

Appendix A

- Figure 6.1.1
- Figure 6.1.2
- Figure 6.2.2a
- Figure 6.2.2b
- Figure 6.2.2c
- Figure 6.3.1
- Figure 6.3.2
- Figure 6.3.3
- Figure 6.4.2
- Figure 6.9

Appendix B

- Glossary
- Additional Attributes List
- Data Collection Overview Document

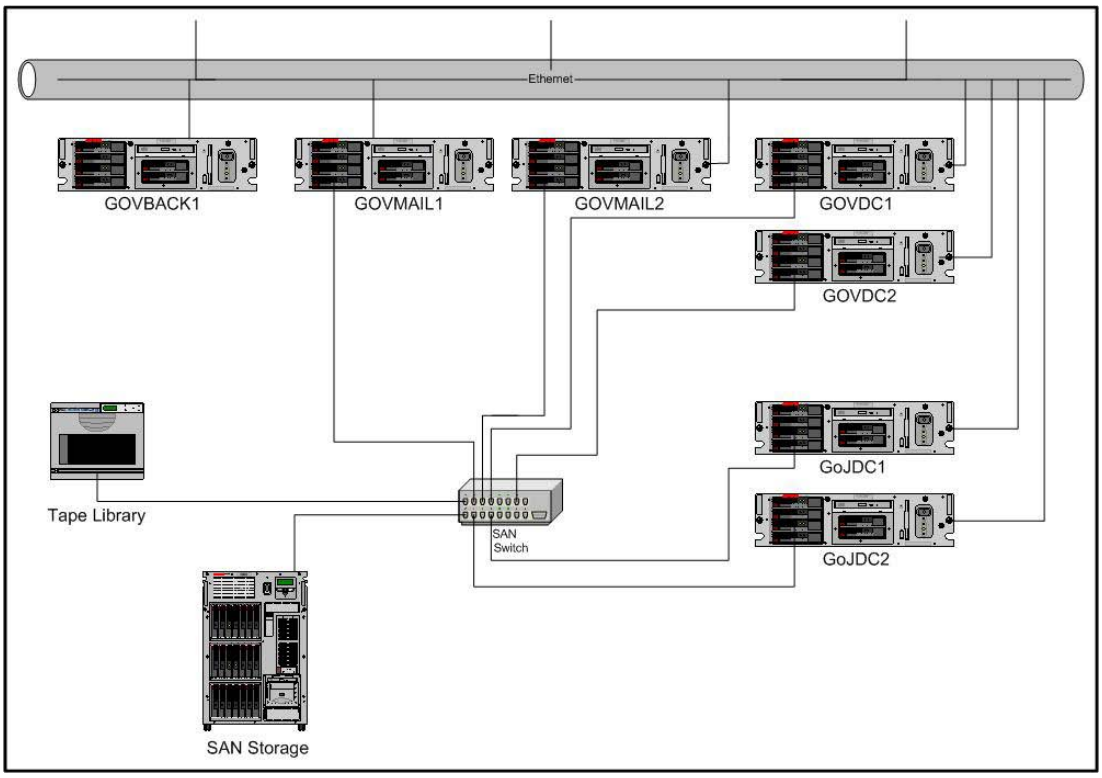


Figure 6.1.1 Physical Layout of the Data Center

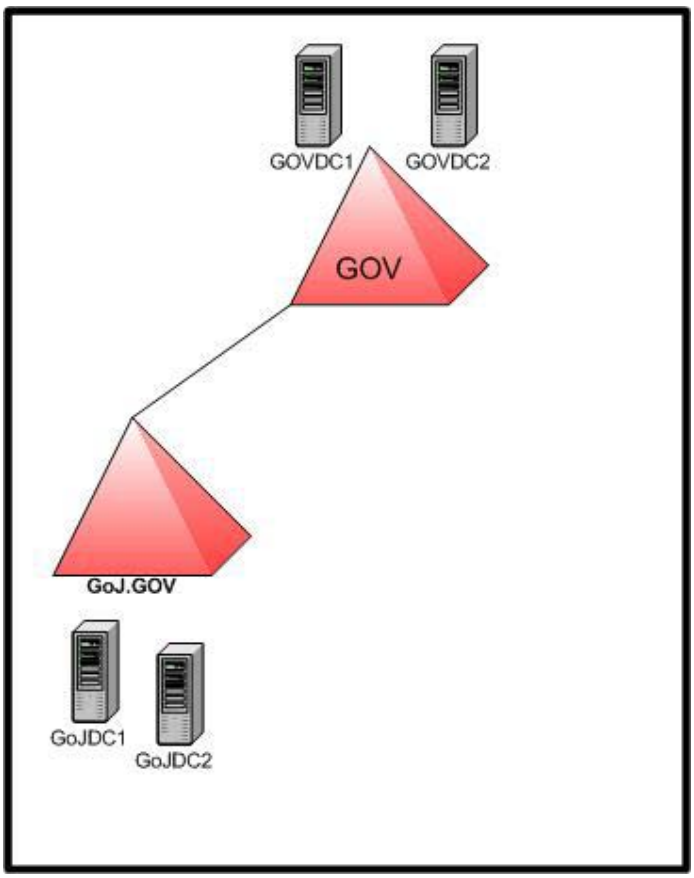


Figure 6.1.2 AD Logical structure in the Data Center

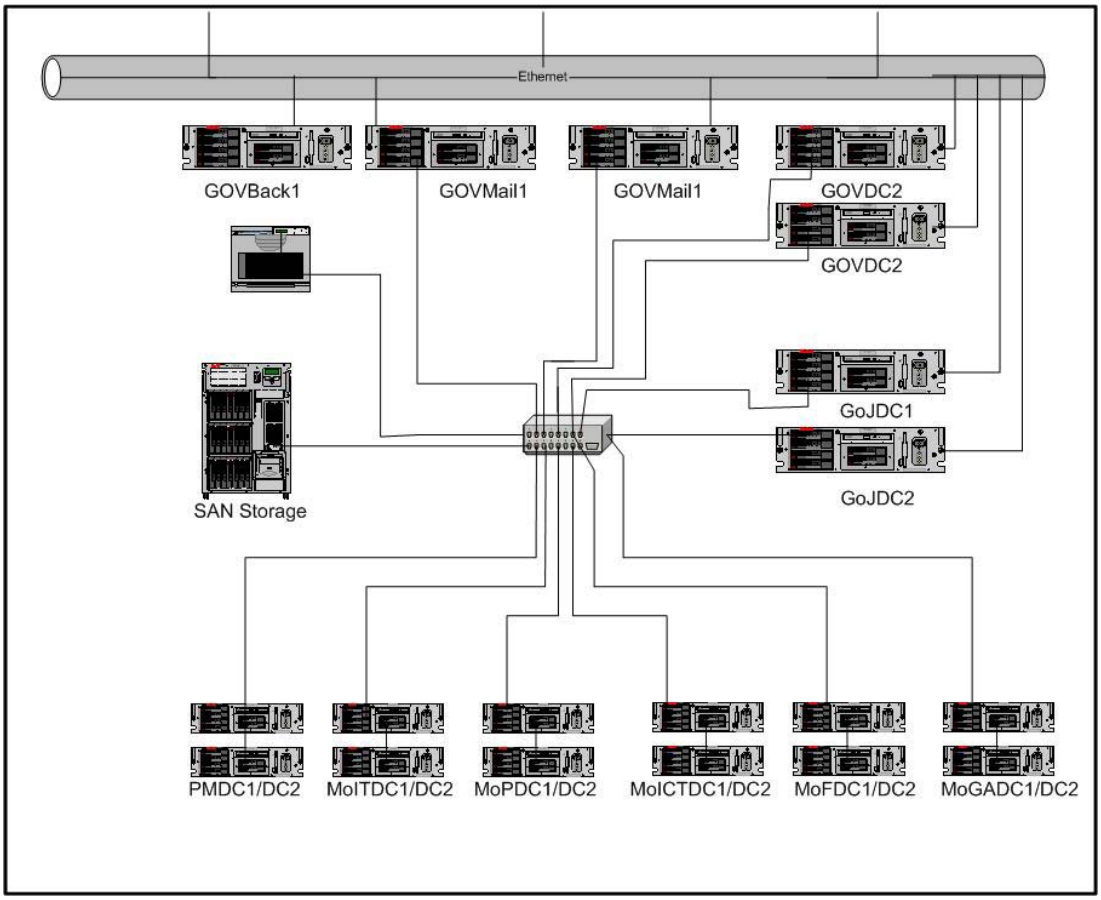


Figure 6.2.2a Physical Layout of the Data Center with Ministries Child Domains

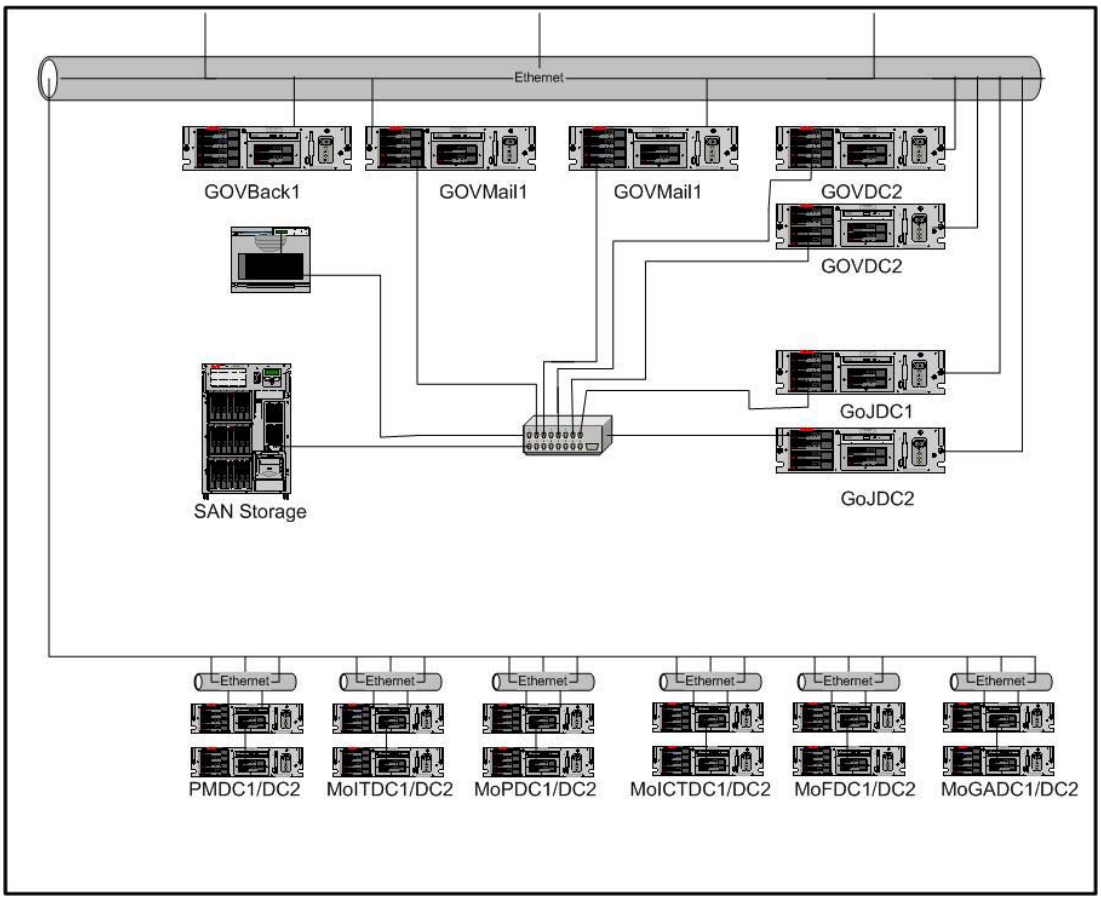


Figure 6.2.2b Physical Layout of the Data Center with Ministries Child Domains

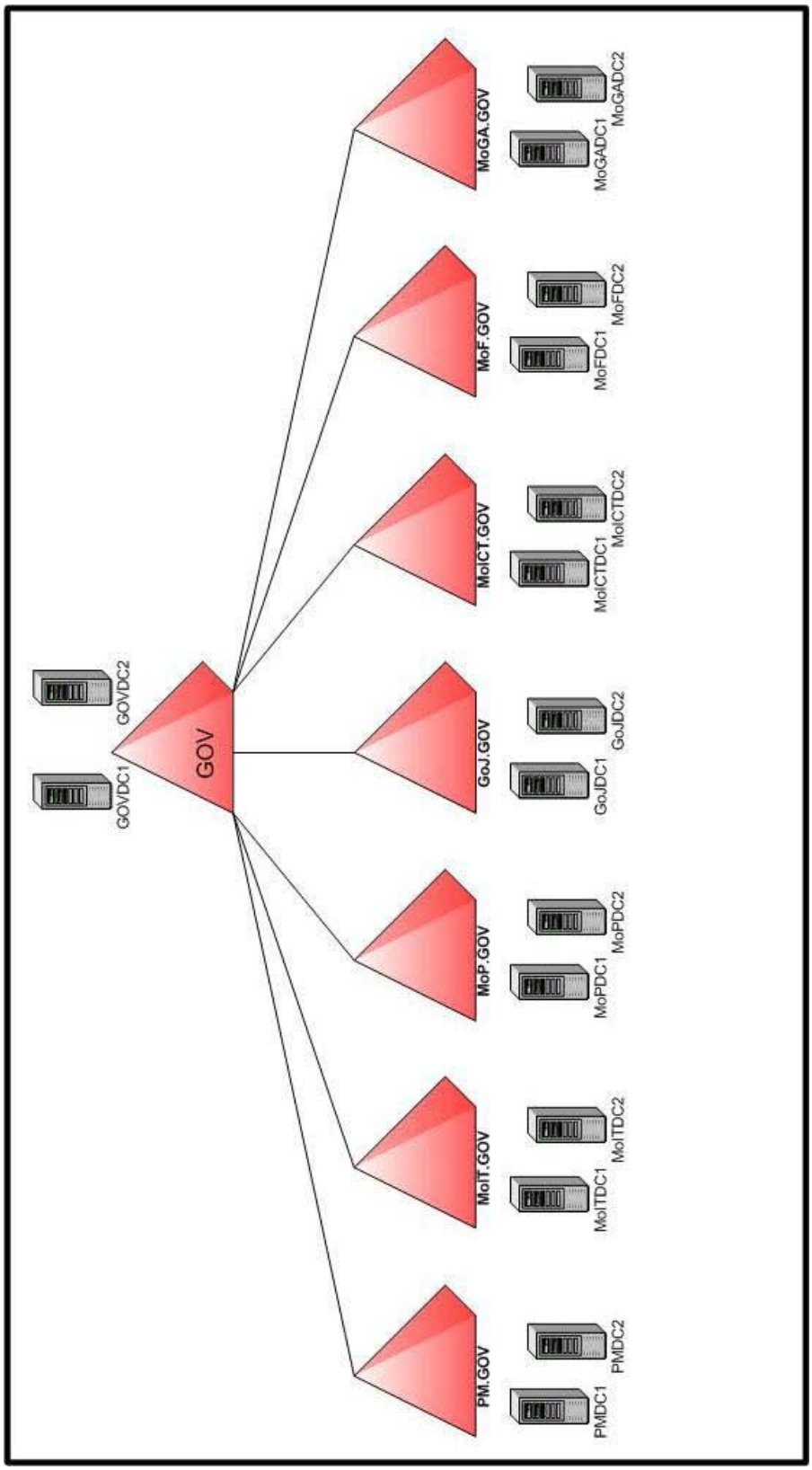


Figure 6.2.2c Logical Layout of the Data Center with Ministries Child Domains

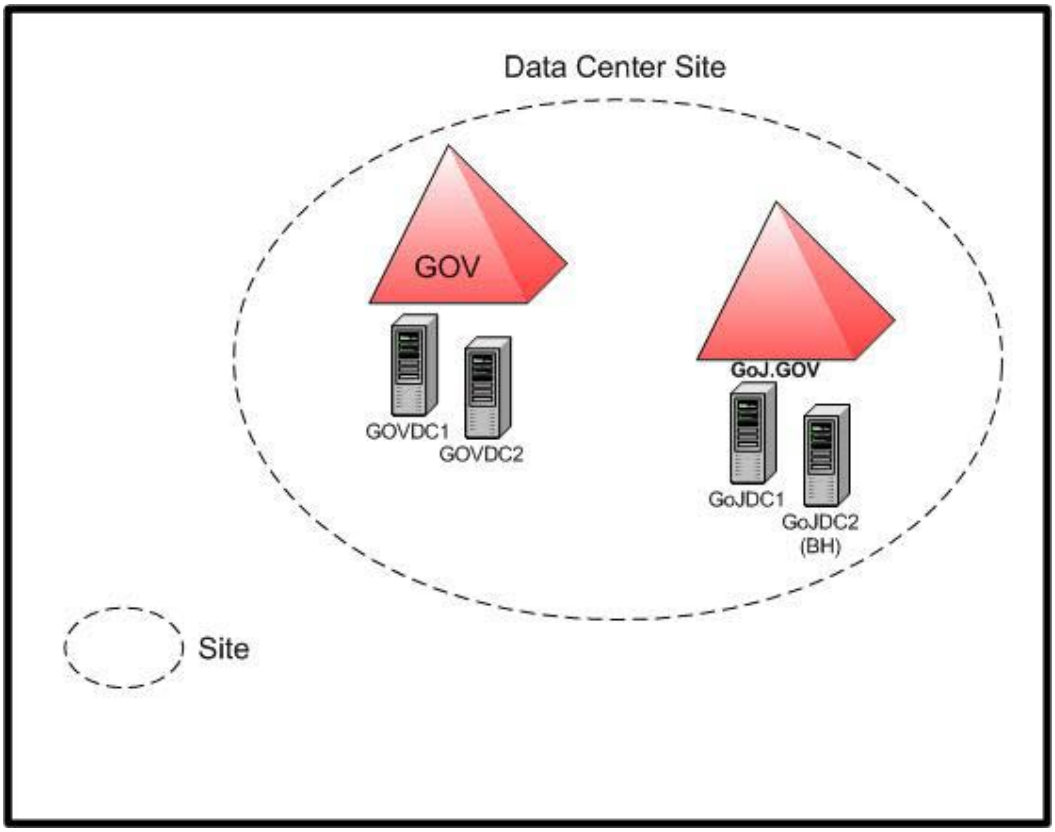


Figure 6.3.1 Active Directory Layout for Single Child Domain Site

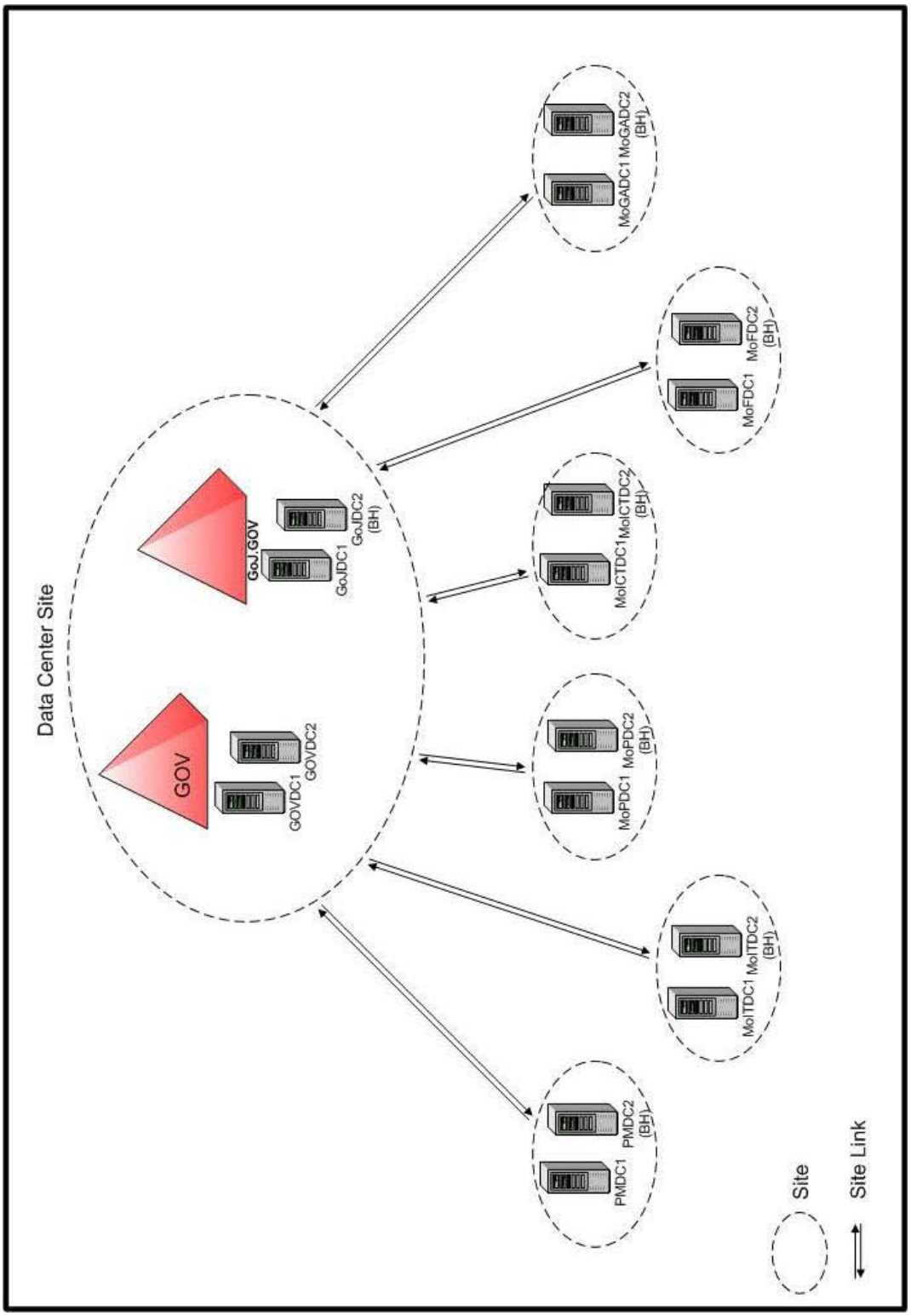


Figure 6.3.2 Active Directory Layout for Multi Child Domains & multi Sites

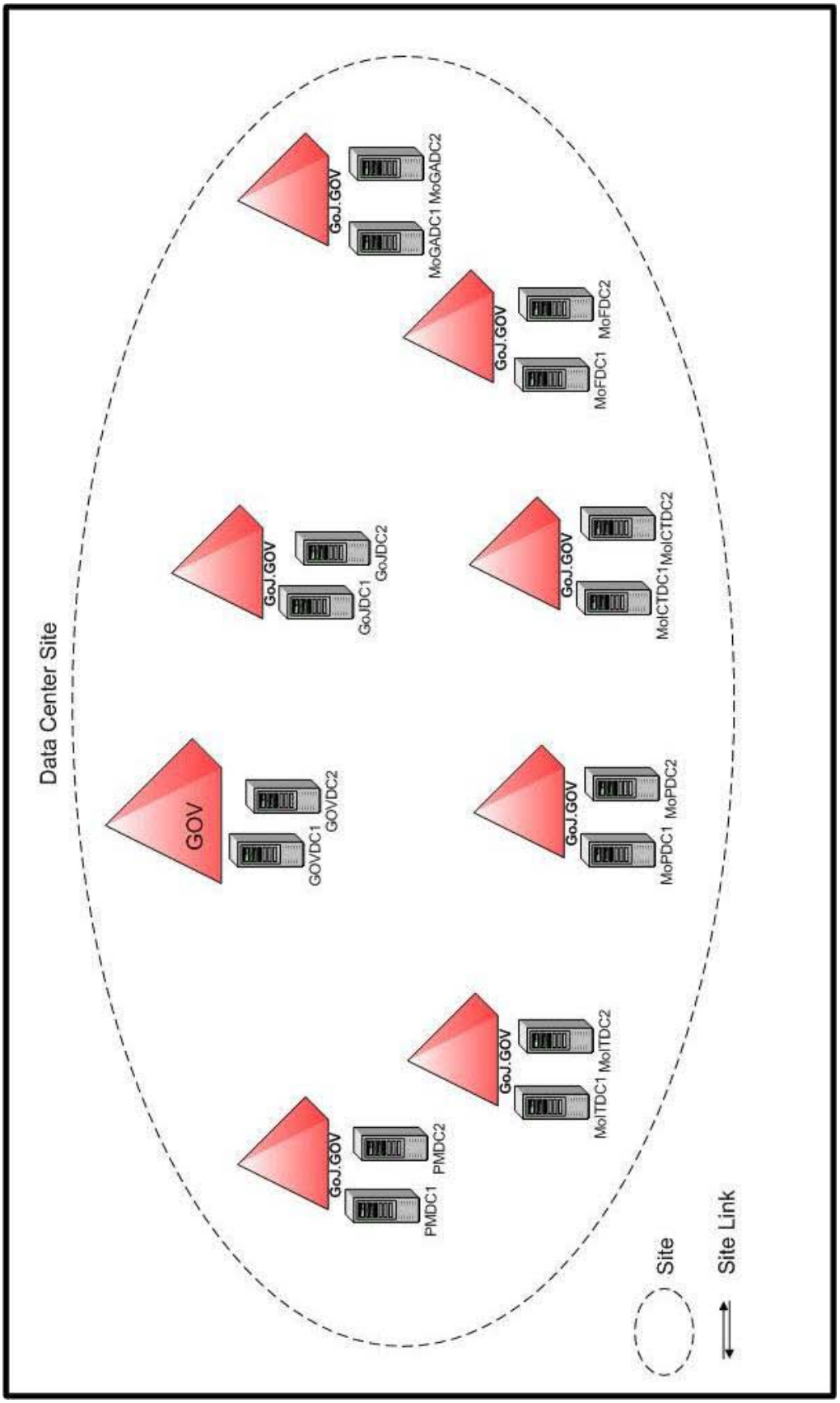
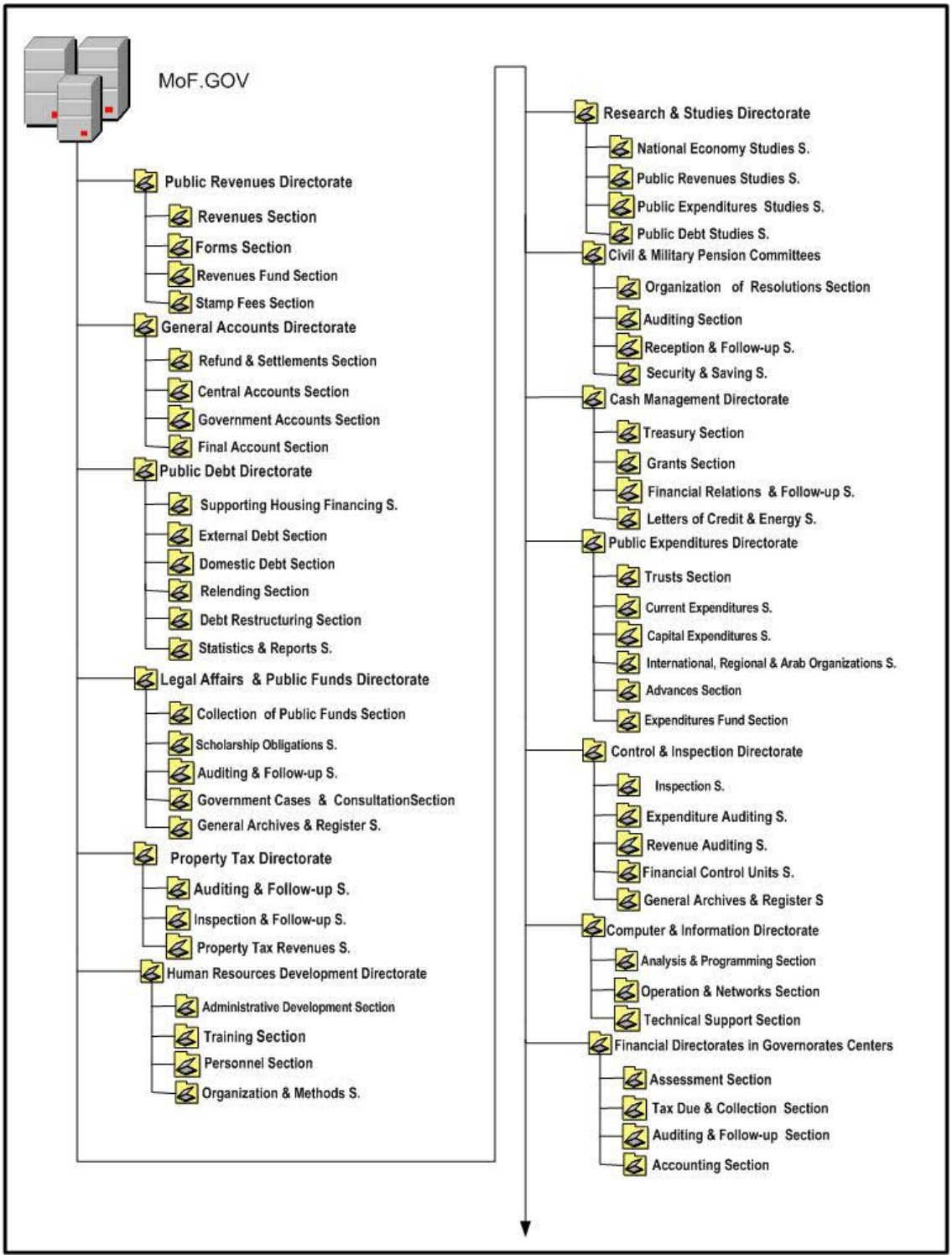


Figure 6.3.2 Multi Child Domains & Single Sites


MoF.GOV
Public Revenues Directorate
Revenues Section
Forms Section
Revenues Fund Section
Stamp Fees Section
General Accounts Directorate
Refund & Settlements Section
Central Accounts Section
Government Accounts Section
Final Account Section
Public Debt Directorate
Supporting Housing Financing S.
External Debt Section
Domestic Debt Section
Relending Section
Debt Restructuring Section
Statistics & Reports S.
Legal Affairs & Public Funds Directorate
Collection of Public Funds Section
Scholarship Obligations S.
Auditing & Follow-up S.
Government Cases & ConsultationSection
General Archives & Register S.
Property Tax Directorate
Auditing & Follow-up S.
Inspection & Follow-up S.
Property Tax Revenues S.
Human Resources Development Directorate
Administrative Development Section
Training Section
Personnel Section
Organization & Methods S.
Research & Studies Directorate
National Economy Studies S.
Public Revenues Studies S.
Public Expenditures Studies S.
Public Debt Studies S.
Civil & Military Pension Committees
Organization of Resolutions Section
Auditing Section
Reception & Follow-up S.
Security & Saving S.
Cash Management Directorate
Treasury Section
Grants Section
Financial Relations & Follow-up S.
Letters of Credit & Energy S.
Public Expenditures Directorate
Trusts Section
Current Expenditures S.
Capital Expenditures S.
International, Regional & Arab Organizations S.
Advances Section
Expenditures Fund Section
Control & Inspection Directorate
Inspection S.
Expenditure Auditing S.
Revenue Auditing S.
Financial Control Units S.
General Archives & Register S
Computer & Information Directorate
Analysis & Programming Section
Operation & Networks Section
Technical Support Section
Financial Directorates in Governorates Centers
Assessment Section
Tax Due & Collection Section
Auditing & Follow-up Section
Accounting Section

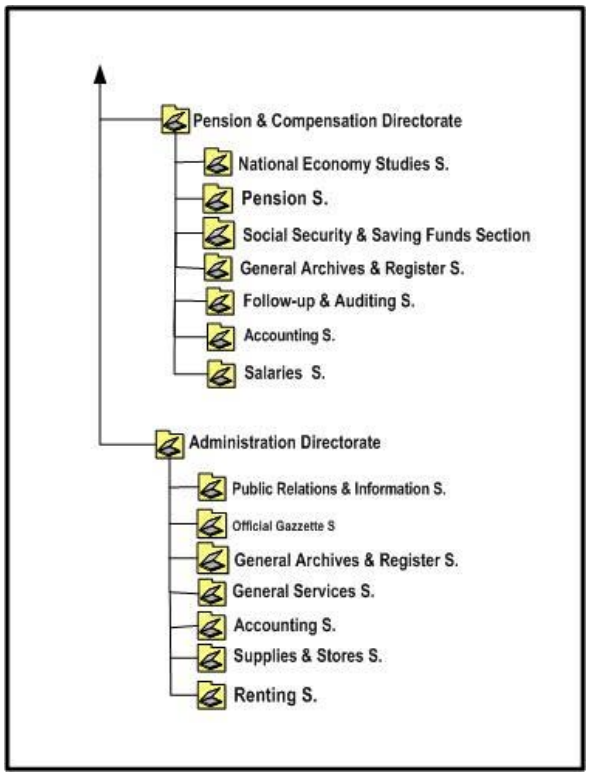


Figure 6.4.2 Ministry of Finance (MOF) Domain OU Structure

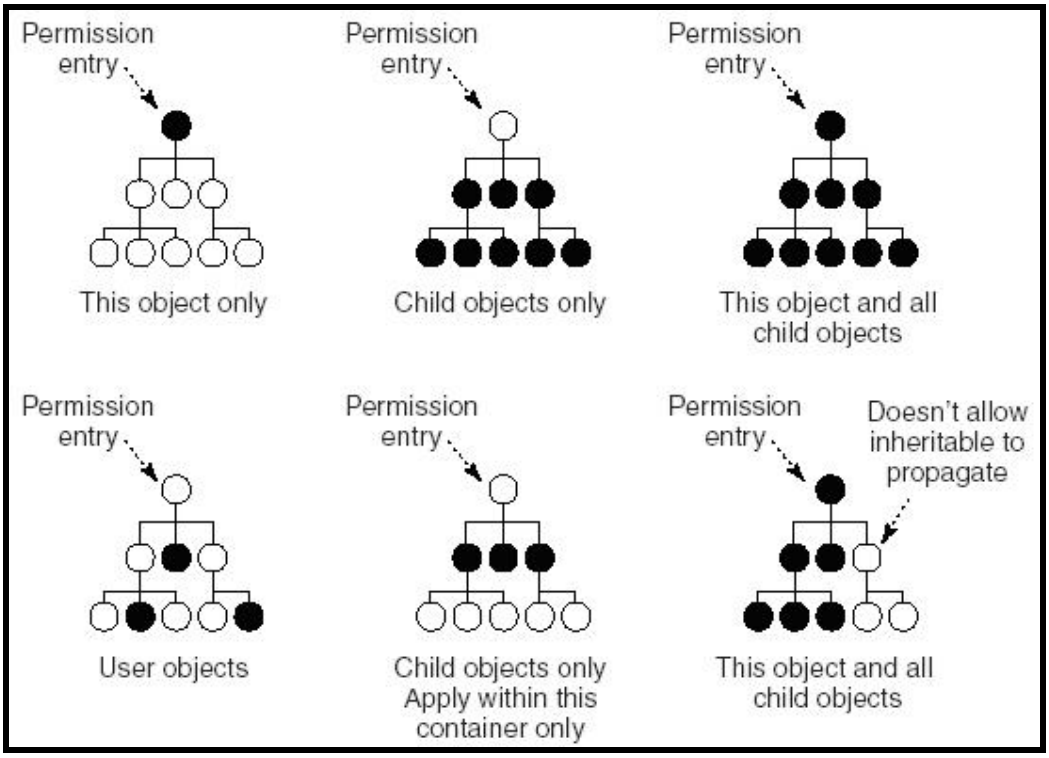


Figure 6.9 AD Object Security Examples

Glossary

•**Schema**
The Active Directory *schema* contains the definitions of all objects, such as computers, users, and printers that are stored in Active Directory. In Windows 2000, there is only one schema for an entire forest, so that all objects created in Active Directory conform to the same rules.

•**Domain**
The core unit of the logical structure in Active Directory is the domain. A *domain* is a collection of computers, defined by an administrator, which share a common directory database. A domain has a unique name and provides access to the centralized user accounts and group accounts maintained by the domain administrator.

•**Domain Controller (DC)**
A *domain controller* is a computer running Windows 2000 Server that stores a replica of the directory service. A domain controller also manages the changes to directory information and replicates these changes to other domain controllers in the same domain. Domain controllers store directory data and manage user logon processes, authentication, and directory searches. A domain controller can be promoted and demoted through the Dcpromo utility.

A domain can have one or more domain controllers. A small organization that uses a single local area network (LAN) may need only one domain with two domain controllers to provide adequate availability and fault tolerance, whereas a large organization with many geographical locations needs one or more domain controllers in each location to provide adequate availability and fault tolerance.

•**Organizational Unit (OU)**
An *organizational unit* is a container object that you use to organize objects within a domain. An OU may contain objects, such as user accounts, groups, computers, printers, and other OUs. It is also a security boundary in that it can have multiple policies applied to it.

•**Tree**
A *tree* is a hierarchical arrangement of Windows 2000 domains that share a contiguous namespace, such as *microsoft.com*, *sales.microsoft.com* and *support.microsoft.com.* When you add a domain to an existing tree, the new domain is a child domain of an existing parent domain. The name of the child domain is combined with the name of the parent domain to form its DNS name. Every child domain has a two-way, transitive trust relationship with its parent domain.

•**Forest**
A *forest* is one or more trees. The trees in a forest do not share a contiguous namespace. However, the trees in a forest share a common schema and global catalog. A single tree that is related to no other trees constitutes a forest of one tree. Thus, every tree root domain has a transitive trust relationship with the forest root domain. The name of the forest root domain is used to refer to a given forest.

Two-Way, Transitive Trusts
Two-way, transitive trust relationships are the default trust relationships between Windows 2000 domains. A two-way, transitive trust is a combination of a transitive trust and a two-way trust.

A *transitive trust* means that the trust relationship extended to one domain is automatically extended to all other domains that trust that domain. For example, domain *sales.microsoft.com* directly trusts *microsoft.com* Domain, *support.microsoft.com* also directly trusts *microsoft.com*. Because both trusts are transitive, *sales microsoft.com* indirectly trusts support.*microsoft.com*.

A *two-way trust* means that there are two trust paths going in opposite directions between two domains. For example, domain *sales. microsoft.com* trusts *microsoft.com* in one direction, and *microsoft.com* trusts *sales.microsoft.com* in the opposite direction. The advantage of two-way, transitive trusts in Windows 2000 domains is that there is complete trust between all domains in an Active Directory domain hierarchy.

•Global Catalog (GC)
The *global catalog* is a repository of information that contains a subset of the attributes of all objects in Active Directory. By default, the attributes that are stored in the global catalog are those that are most frequently used in queries, such as a user's first name, last name, and logon name, etc.
The first domain controller you create in a domain automatically becomes the global catalog server. You can configure additional global catalog servers to balance the traffic from logon authentication and queries.

The global catalog also contains the access permissions for each object and attribute stored in the global catalog. If you are searching for an object and you do not have the appropriate permissions to view the object, you will not see the object in the list of search results. This ensures that users can find only objects to which they have been assigned access.

The attributes that are tagged for replication to the Global Catalog are assigned through the Active Directory Schema Manager Microsoft Management Console (MMC) snap-in. There is only one *policy* for Global Catalog attribute replication in the forest. A Global Catalog will listen on port 3268 for LDAP queries (that are global to the forest), and port 389, which standard domain controllers use (for local domain queries).A domain controller can be made into a Global Catalog (and vice versa) by selecting or deselecting a check box in the Active Directory Sites and Services MMC snap-in.

•Schema Master Role
The *schema master* controls all originating updates to the schema. The domain controller that holds the schema master role is the only domain controller that can perform write operations to the directory schema. These schema updates are replicated from the schema operations master to all other domain controllers in the forest. Having only one schema master per forest prevents any conflicts that would result if two or more domain controllers attempt to concurrently update the schema. Only the Schema Admins group can make modifications to the schema.

•**Domain Naming Master Role**
The *domain naming master* controls the addition or removal of domains in the forest. There is only one domain naming master per forest. When you add a new domain to the forest, only the domain controller holding the domain naming master role has the right to add the new domain. The domain naming master manages this process, preventing multiple domains from joining the forest with the same domain name. When you use the Active Directory Installation wizard to create a child domain, it contacts the domain naming master and requests the addition or deletion. The domain naming master is responsible for ensuring that the domain names are unique. Note that if the domain naming master is unavailable, you cannot add or remove domains.

•**Primary Domain Controller (PDC) Emulator Role**
The *PDC emulator* acts as a Microsoft Windows NT® PDC to support any backup domain controllers (BDCs) running Windows NT within a mixed-mode domain. The PDC emulator is the first domain controller that is created in a new domain.

•**Relative Identifier Master Role**
The *relative identifier (RID) master* allocates blocks of RIDs to each domain controller in the domain. Whenever a domain controller creates a new security principal, such as a user, group, or computer object, it assigns the object a unique security identifier (SID).

•**Infrastructure Master Role**
The *infrastructure master* is used to update object references in its domain that point to the object in another domain. The object reference contains the object's globally unique identifier (GUID), distinguished name and possibly a SID. The distinguished name and SID on the object reference are periodically updated to reflect changes made to the actual object. These changes include moves within
and between domains as well as the deletion of the object.

•**Site**
A *site* consists of one or more Internet Protocol (IP) subnets that are connected by a high-speed link. By defining sites, you can configure the access and replication topology for Active Directory so that Windows 2000 uses the most efficient links and schedules for replication and logon traffic. Multiple sites may exist within a single domain, and conversely, a single site may span multiple domains.

•**User Principal Name (UPN)**
This is a unique method of identifying each user across a forest and typically equates to an email address like user@mof.gov.jo. A UPN allows the underlying domain structure and complexity to be hidden from users; for example, although 50 domains may exist within a forest, users would seamlessly log on as if they were in the same domain.

Additional Attributes Lists

1- Attributes for the User class are:

- First Name
- الأسم الأول
- Second Name
- اسم الأب
- Third Name
- أسم الجد
- Family Name
- اسم العائلة
- Directorate/Unit
- الوحدة/المديرية
- Job Title
- المسمى الوظيفي
- Job Description
- الوصف الوظيفي
- National ID Number
- الرقم الوطني
- Office Phone Number
- هاتف العمل
- Office Phone Extension
- فرعى
- Direct Phone Number
- هاتف مباشر
- Office Fax Number
- فاكس العمل
- Work Mobile
- هاتف نقال
- Home Phone Number
- هاتف المنزل
- E-Mail
- البريد الألكتروني
- Gender
- الجنس
- Employee Photo
- صورة الموظف
- Salutation
- صيغة التخاطب/اللقب الرسمي
- Location of Department
- موقع الدائرة

2- Attributes for the OU class are:

- Name
- الأسم
- Description
- E-mail Address
- البريد الألكتروني
- Web Site
- الموقع الألكتروني

- Telephone Number
- هاتف العمل
- Fax Number
- فاكس العمل
- Street Address
- العنوان
- P.O Box
- صندوق البريد
- Postal Code
- الرمز البريدي
- City
- المدينة
- Country
- البلد
- Working Hours
- ساعات العمل
- Working Days
- ايام العمل
- 1st Contact Person
- 2nd Contact Person
- URL

E-Government Portal

Data Collection Overview Document
For
Enterprise Directory, Personnel Directory and Organization Directory

1.1.1 Copies to:

Name	Medium (Fax, E-mail, etc)
STS Data Collection Team	**eyad@sts.com.jo**
Other IQC Data Collection Teams	**E-Mail**
MoICT – Fadi Mer3y	**E-mail**

Attachments:

None

Document Control

Author:	Eyad Suboh
Modified By (list):	Sadek Shunnar
Reviewed By:	

Objective:

The purpose of this document is to collect specific information about the government ministries in order to establish the design for Enterprise, Personnel, and Organization Directories that are part of the E-Government Portal Web Sites.

Required Information:

As your ministry part of this project and we all are working as one team to reach the big picture, the following information is required to be collected:

- Organization Information structure
- Personnel Information
- Current Network Infrastructure and Network Operating System

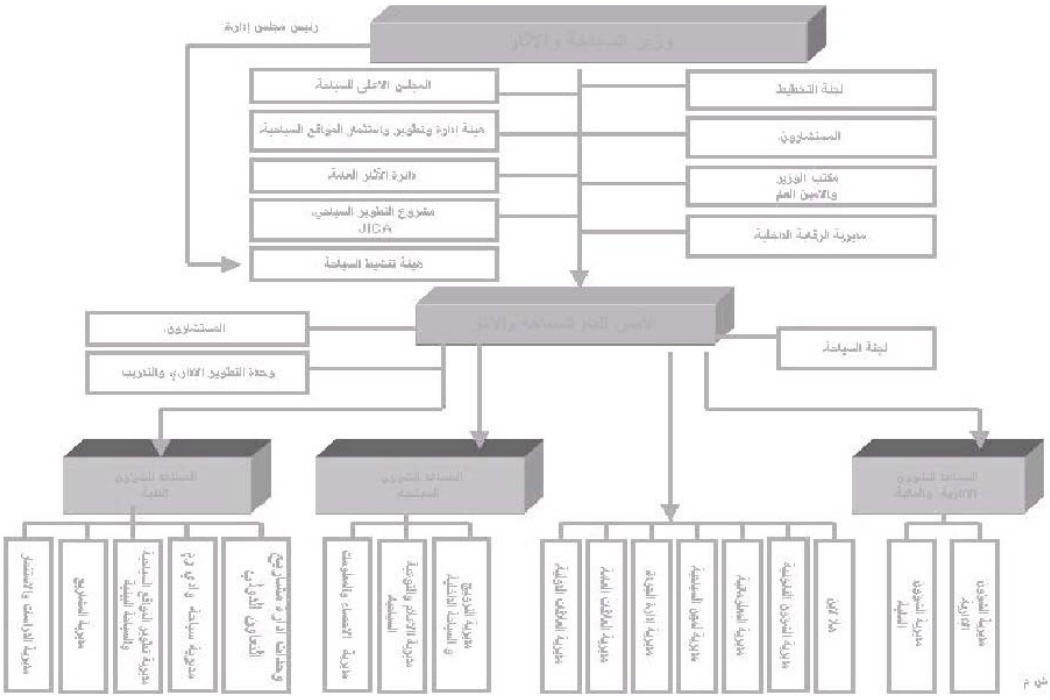
Details:

- **Organization Structure**

Each ministry has its own organization structure that maps the ministry hierarchal structure (see example next page). We will require having your input for your ministry/institute hierarchal structure, in an electronic format (Word, OrgChart, Visio... etc). The type of information needed should contain:

- Hierarchy of the Ministry/institute and its sub organization units (Sections, Offices, Centers, Departments, etc.). Please note that if a Department is part of the ministry/institute hierarchy, we'd also require getting its information, either directly with your ministry/institute or by visiting them for the same.
- Name and Title for all departments and divisions (Arabic/English).
  - A Brief paragraph explaining the department responsibility (description of activity) in one line
  - Arabic Name
  - English name
- Contact information for each Organization Unit :
  - Telephone number(s), … *if there is more than one number please add it to the templates*
  - Fax number(s)
  - Mailing Address, … *If there is more than one e-mail address please add it to the templates*
  - Street address, … *(Area, Block, St, Bldg, Appt ...)*
  - Contact for PR officer if any,
  - Public email(s) of the ministry & a description of purpose
  - Website

** The required information should be in Arabic and English languages


رئيس مجلس إدارة
وزير السياحة والآثار
المجلس الأعلى للسياحة
هيئة إدارة وتطوير واستثمار المواقع السياحية
دائرة الآثار العامة
مشروع التطوير السياحي JICA
هيئة تنشيط السياحة
لجنة التخطيط
المستشارون
مكتب الوزير والأمين العام
مديرية الرقابة الداخلية
المستشارون
وحدة التطوير الاداري والتدريب
لجنة السياحة

❖ **Personnel Information**

Personal and business information for the government employees in each unit in the ministry/institute is required for building the Personnel Directory of the G2G Portal Site. This will also be the basis for the Enterprise Directory users whom will be part of the SGN.

Such information is needed to be in relation to the Organization Unit the employee belongs to. (the Organization Unit he/she works for). This should be mapped within the above organization structure.

The type of information needed should contain:

- Full name of the employee from four parts, in English and Arabic
- Job Title, in English and Arabic
- Brief Job Description, in Arabic and English
- ** The Organization Unit he/she works for
- Work Telephone Numbers & extension
- Work Fax Number (if Private fax)
- Work Mobile Number
- Optional
  - Home Phone number
  - Employee Photo

** The required information should be in Arabic and English languages

❖ **Network Infrastructure and OS**

In order to introduce your ministry/institute to the SGN & its applications, it's required to capture the exact Network & Operating System Infrastructure within. The type of information needed should contain:

- Layout Diagram of the Network
  - Infrastructure
  - Network Services type
- Domain & Application Servers listing (All types Servers in general)
  - Operating System version
  - Installed Applications & Packages
- Print & File Servers listing
  - Operating System version
  - Installed Applications & Packages
- Internet Access and firewalls, if any
  - Operating System
  - Firewall type
  - Proxy type, if any
  - Name of ISP